UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,461	03/31/2004	Moinul H. Khan	884.B89US1	6391

21186 7590 07/17/2008
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
SHAIFER HARRIMAN, DANT B	
ART UNIT	**PAPER NUMBER**
2134	
MAIL DATE	**DELIVERY MODE**
07/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/815,461	**Applicant(s)** KHAN ET AL.	
	Examiner DANT B. SHAIFER HARRIMAN	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _11 June 2008_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1 -32_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1 - 32_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _31 March 2004_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

Response to Amendment

Status of the instant application:

- Claims 1 - 32 are original in the instant application.
- No claims have been amended in the instant application.
- No claims have been cancelled in the instant application.
- Referring to claims 1 – 5 & 6 - 13 under the 35 U.S.C. 101 rejection, applicants remarks and arguments concerning the rejection have been fully considered and are not persuasive. Please see the office action below for details.
- Applicant's amendments to the disclosure of the missing serial number have been considered and are persuasive, and the corresponding objection to the disclosure is withdrawn.

Response to Arguments

- Applicants arguments/remarks filed 06/11/2008 have been fully considered and are not persuasive.

Examiner response to applicant's arguments/remarks:

Applicant states: "This section of Dariel does not disclose that the controller is to preclude execution of an operation if a condition is not met."

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to Col. 3, lines 63 – 67 & Col. 7, lines 28 – 36, Figure #2, component # 16, the examiner notes that the examiner equates "if the condition is not met," with whether or not the ASIC (Application specific integrated circuit) which contains the processor or cryptoprocessors are authenticated by the server # 50 or not, with that said, the "preclude execution of an operation" is equated with the ASIC or processor or controller going to receiving the requested encrypted content from the server #50.

Applicant states: "Specifically, this section of Dariel does not disclose that the controller is to preclude execution of a sensitive operation if the apparatus is within an untrusted state. "

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to Col. 3, lines 63 – 67 & Col. 7, lines 28 – 36, Figure #2, component # 16, the examiner notes that the examiner equates "if the apparatus is within an untrusted state," with whether or not the ASIC (Application specific integrated circuit) which contains the processor or cryptoprocessors are authenticated by the server # 50 or not, with that said, the "preclude execution of a sensitive operation" is equated with the ASIC or processor or controller going to receiving the requested encrypted content from the server #50.

Applicant states: "Because Dariel does not disclose each element of claims 1, 6 and 19, Applicant respectfully submits that the rejection of claims 1, 6 and 19 under 35 U.S.C. §102 has been overcome. "

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to the examiners previous logic and reasoning above.

Applicant states: "This section of Howard does not disclose any type of validation of a cryptographic key. Specifically, this section of Howard does not disclose validation of a cryptographic key based on a hash that is stored in a one time programmable storage in a memory that is external to the cryptographic processor. "

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to Col. 5, lines 40 – 67 & Col. 6, lines 1 – 18, the examiner notes that the examiner equates "validation of a cryptographic key based on a hash," with key seed k1, and first seed s1 from the first device, and second seed s2 from the second device to make a key # 320 that is provided to either the encryption logic or decryption logic of either device, furthermore the "one time programmable storage in memory that is external to the cryptographic processor, is equated with that the cryptoprocessors are on the first device, and the hash unit is in the memory of the second device that is external to the first device, the hash unit in the second device is one time programmable in the sense that the hash only produces a second seed s2 # 318, that is used in the hashing process.

Applicant states: “Because Howard does not disclose each element of claims 14 and 23, Applicant respectfully submits that the rejection of claims 14 and 23 under 35 U.S.C. § 102 has been overcome.”

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to the examiners previous logic and reasoning above.

Applicants states: “However, these sections of Zotto do not disclose any type of validation. ”

- The examiner respectfully disagrees with applicants logic and reasoning, te examiner points to paragraphs 0034, 0035, 0036 of Zotto, the examiner notes that a hash of the requested content is made at the content source # 106, and then when the requested content is sent to the game console, the game sole will also compute a hash and then compare the hash of the content source # 10 6 with its own hash, if the hash's match, then the request content has not been tampered with. Thus is how the Zotto prior art discloses validation.

Applicants states: “Specifically, these sections of Zotto do not disclose a controller to validate a patch based on the cryptographic key and the hash of the cryptographic key.”

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to paragraphs 0034, 0035, 0036 of Zotto, the examiner notes that the examiner interprets patch as the requested game content from the content source # 106, also the controller can be both the content source # 106 and the game console # 102, the validation is equal to how that a hash (i.e. cryptographic key) of the requested content is made at the content source # 106, and then when the requested content is sent to the game console, the game sole will also compute a hash and then compare the hash of the content source # 10 6 with its own hash, if the hash's match, then the request content has not been tampered with.

Applicants states: "Because Howard does not disclose each element of claim 27, Applicant respectfully submits that the rejection of claim 27 under 35 U.S.C. § 102 has been overcome."

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to the examiners previous logic and reasoning above.

Specification

1. The disclosure is objected to because of the following informalities: the applicant's summary is missing.
Appropriate correction is required.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 1 – 5 & 6 -13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims(s) 1 – 5 & 6 - 13 are directed to cryptographic processor, that contains a non-volatile memory, program instructions, a controller.

This claimed subject matter lacks a practical application of a judicial exception (law of nature, abstract idea, naturally occurring phenomenon) since it fails to produce a useful, concrete and tangible result.

Specifically, the claimed subject matter does not produce a tangible result because the claimed subject matter fails to produce a result that is limited to having real world value rather than a result that may be interpreted to be abstract in nature as, for example, a thought, a computation, or manipulated data. More specifically, the claimed subject matter provides for the above mentioned claims recite claim limitations that are conditional in nature, meaning that "if event (Z) happens then event (X) will be executed.” Then what if event (Z) doesn't happen, then event (X) will not happen. The examiner point is, if event (Z) doesn’t happen, then nothing **tangible** is happening to event (X), which would be "executing event (X),” Specifically, the examiner notes that the independent claim is only tangible if the "at least one microcode instruction if the microcode is not a sensitive operation," otherwise if the micro instruction code is **not** a sensitive operation, then the examiner concludes that the instructional microcode is just sitting in memory (non - volatile), being **not tangible**.

This produced result remains in the abstract and, thus, fails to achieve the required status of having real world value.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim(s) 1 – 13 & 19 – 22 are rejected under 35 U.S.C. 102(e) as being taught by Dariel (US Patent # 7058818 B2).

Dariel teaches:

Claim # 1. An apparatus comprising:

a cryptographic processor within a wireless device, the cryptographic processor comprising:

- at least one cryptographic unit (Col. 3, lines 20 – 22 & Col. 3, lines 28 – 34 & Col. 3, lines 38 – 47 & Col. 3, lines 48 – 67 & Col. 4, lines 19 – 25 & Col. 6, lines 16 - 27);

- a nonvolatile memory to store one or more microcode instructions, wherein at least one of the one or more microcode instructions is related to a sensitive operation(Col. 4, lines 26 – 30 & Col. 4, lines 50 – 52, the examiner notes that ROM is a type of non-volatile memory); and

- a controller to control execution of the one or more microcode instructions by the at least one cryptographic unit, wherein the controller is to preclude execution of the sensitive operation if the apparatus is within an untrusted state(Col. 7, lines 28 – 36 & Figure #2, component # 16, the examiner notes that the digital video and audio are encrypted, which leads the examiner to the assumption that the cryptographic processor is operating in an "untrusted" state).

Claim # 2.The apparatus of claim 1, further comprising:

- a volatile memory to store a cache of at least one cryptographic key and a counter, and at least one platform configuration register(Col.6, lines 20 – 25, the cryptographic processor uses RAM for decryption key storage purposes).

Claim # 3. The apparatus of claim 2, wherein a sensitive operation is an operation that uses a root encryption key for the apparatus, an operation that uses one of the at least one

- encryption key(Col.6, lines 20 – 25, the cryptographic processor uses RAM for decryption of encrypted digital data and storage purposes) or

- an operation that is to access the counter() or
- the at least one platform configuration register ().

Claim # 4. The apparatus of claim 2, wherein

- the apparatus is within the untrusted state
    - if the apparatus is improperly initialized,
    - if an authentication operation of one of the at least one cryptographic key fails (Col. 3, lines 63 - 67 & Col. 7, lines 20 - 26, the examiner notes that if the circuit is not authenticated by the server, then the ASIC will not receive the encrypted digital audio and video data or the decryption keys) or
    - if one of the cryptographic units is to perform an illegal operation.

Claim # 5. The apparatus of claim 4, wherein

- an illegal operation includes an out-of- order execution by one of the at least one cryptographic units (Col. 3, lines 63 - 67 & Col. 7, lines 20 - 26, the examiner notes that if the circuit is not authenticated by the server and the circuit requested the digital data, then the ASIC (application specific integrated circuuit) will not receive the encrypted digital audio and video data or the decryption keys).

Claim # 6. A method comprising:

- receiving a primitive instruction into a cryptographic processor within a wireless device(Col. 7, lines 39 – 42, the examiner notes that the user wishes to play the encrypted digital data, the examiner interprets this action as the cryptographic processor receiving a primitive instruction, furthermore the examiner notes that the term "primitive instruction" is just merely data.);

- retrieving at least one microcode instruction from a nonvolatile memory within the cryptographic processor based on the primitive instruction (Col. 7, lines 39 – 42, the examiner notes that the decryption keys are retrieved from flash memory); and

- executing the at least one microcode instruction if the microcode instruction is not a sensitive operation or if the at least one microcode instruction is a sensitive operation and the cryptographic processor is in a trusted state (Col. 7, lines 39 – 42, the examiner notes that the user instructs the cryptographic processor and corresponding controller # 16 to retrieve the encrypted data and corresponding decryption key, which will be used to decrypt the encrypted digital data, this is what the examiner considers as a non-sensitive operation).

Claim # 7. The method of claim 6, wherein

- executing the at least one microcode instruction if the microcode instruction is not the sensitive operation comprises executing the at least one microcode instruction if the microcode instruction does not uses a root encryption key of the cryptographic processor(Col. 7, lines 39 – 42, the examiner notes that the user instructs the cryptographic processor and corresponding controller # 16 to retrieve the encrypted data and corresponding decryption key, which will be used to decrypt the encrypted digital data, this is what the examiner considers as a non-sensitive operation).

Claim # 8. The method of claim 6, wherein

- executing the at least one microcode instruction if the microcode instruction is not the sensitive operation comprises executing the at least one microcode instruction if the microcode instruction does not uses an encryption key protected within the cryptographic processor (Col. 3, lines 63 - 67 & Col. 7, lines 20 - 26, the examiner notes that the ASIC must request to be authenticated by the server before the release of the encrypted digital data, this is what the examiner considers as a non-sensitive operation).

Claim # 9. The method of claim 6, wherein

- executing the at least one microcode instruction
    - if the microcode instruction is not the sensitive operation comprises executing the at least one

microcode instruction (Col. 7, lines 39 – 42, the examiner notes that the user instructs the cryptographic processor and corresponding controller # 16 to retrieve the encrypted data and corresponding decryption key, which will be used to decrypt the encrypted digital data, this is what the examiner considers as a non-sensitive operation)

- if the microcode instruction does not access a monotonic counter or data in a platform configuration register().

Claim # 10. The method of claim 6 further comprising

- initializing the cryptographic processor prior to receiving the primitive instruction (Col. 6, 7 – 12 & Col. 7, lines 39 – 43, the examiner notes that the user platform is a cellular or mobile telephone that communicates with a sever that is in a remote location juxtaposition to the mobile telephone, furthermore the examiner notes that in order for the user to request the digital content from the remote server, the phone must be on, and since the ASIC, which contains the cryptographic processor is also located in the phone, the cryptographic processor is therefore initialized),

wherein initializing comprises

- verifying at least one functional unit in the cryptographic processor is generating proper results (Col. 3, lines 63 - 67 & Col. 7, lines 20 – 26 & Col. 7, lines 39 – 43, the examiner notes that the "cryptographic processor is generating proper results," when the ASIC is authenticated by the server).

Claim # 11. The method of claim 10, wherein

- verifying the at least one functional unit in the cryptographic processor is generating proper results comprises verifying a hash unit in the cryptographic processor is generating correct hashes (Col. 3, lines 63 - 67 & Col. 7, lines 20 – 26 & Col. 6, lines 55 – 61, the examiner notes that the cryptographic processor or processors can produce hashes, furthermore the examiner notes that the “cryptographic processor is generating correct hashes,” when the ASIC is authenticated by the server).

Claim # 12. The method of claim 10, wherein

- verifying the at least one functional unit in the cryptographic processor is generating proper results comprises verifying a random number generator unit is generating random numbers (Col. 3, lines 63 - 67 & Col. 7, lines 20 – 26 & Col. 6, lines 34 – 39, the examiner notes that the ASIC contains a component that is a random number generator, furthermore the examiner notes that "at least one functional unit in the cryptographic processor is generating proper results comprises verifying a random number generator unit is generating random numbers," when the ASIC is authenticated by the server).

Claim # 13. The method of claim 10, wherein

- verifying the at least one functional unit in the cryptographic processor is generating proper results comprises verifying an exponential arithmetic unit or an arithmetic logic unit is computing proper results (Col. 3, lines 63 - 67 & Col. 7, lines

20 – 26 & Col. 7, lines 39 – 43, the examiner notes that the "cryptographic processor is generating proper results," when the ASIC is authenticated by the server).

Claim # 19.A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

- receiving a primitive instruction into a cryptographic processor (Col. 7, lines 39 – 42, the examiner notes that the user wishes to play the encrypted digital data, the examiner interprets this action as the cryptographic processor receiving a primitive instruction, furthermore the examiner notes that the term "primitive instruction" is just merely data, furthermore the examiner considers the flash memory or

EEPROM as a "machine-readable medium.");

- retrieving at least one microcode instruction from a memory within the cryptographic processor based on the primitive instruction (Col. 7, lines 39 – 42, the examiner notes that the decryption keys are retrieved from flash memory or EEPROM memory); and

- executing the at least one microcode instruction if the at least one microcode instruction is a sensitive operation and the cryptographic processor is in a trusted state (Col. 7, lines 39 – 42, the examiner notes that the user instructs the cryptographic processor and corresponding controller # 16 to retrieve the encrypted data and corresponding decryption key, which will be used to decrypt the encrypted digital data, this is what the examiner considers as a non-sensitive operation).

Claim # 20. The machine-readable medium of claim 19, wherein

- executing the at least one microcode instruction if the microcode instruction is a sensitive operation comprises executing the at least one microcode instruction if the microcode instruction uses a root encryption key of the cryptographic processor (Col. 7, lines 39 – 42, the examiner notes that the user instructs the cryptographic processor and corresponding controller # 16 to retrieve the encrypted data and corresponding decryption key, which will be used to decrypt the encrypted digital data, this is what the examiner considers as a sensitive operation).

Claim # 21. The machine-readable medium of claim 19, wherein

- executing the at least one microcode instruction if the microcode instruction is a sensitive operation comprises executing the at least one microcode instruction if the microcode instruction uses a data encryption key protected within the cryptographic processor (Col. 7, lines 39 – 42, the examiner notes that the user instructs the cryptographic processor and corresponding controller # 16 to retrieve the encrypted data and corresponding decryption key, which will be used to decrypt the encrypted digital data, this is what the examiner considers as a sensitive operation).

Claim # 22. The machine-readable medium of claim 19 further comprising

- initializing the cryptographic processor prior to receiving the primitive instruction, wherein initializing comprises verifying at least one functional unit in the cryptographic processor is generating proper results (Col. 6, 7 – 12 & Col. 7, lines 39 – 43, the examiner notes that the user platform is a cellular or mobile telephone that communicates with a sever that is in a remote location juxtaposition to the mobile telephone, furthermore the examiner notes that in order for the user to request the digital content from the remote server, the phone must be on, and since the ASIC, which contains the cryptographic processor is also located in the phone, the cryptographic processor is therefore initialized, furthermore Col. 3, lines 63 - 67 & Col. 7, lines 20 – 26 & Col. 7, lines 39 – 43, the examiner notes that the “cryptographic processor is generating proper results,” when the ASIC is authenticated by the server).

Claim(s) 14 - 18 & 23 - 26 are rejected under 35 U.S.C. 102(e) as being taught by Howard et al. (US Patent # 7269736 B2).

Howard teaches:

Claim # 14. A method comprising:

- receiving a patch of at least one microcode instruction stored in nonvolatile memory within a cryptographic processor in a wireless device (Col. 2, lines 20 – 25 & Col. 2, lines 31 – 36 & Col. 3, lines 14 – 53 & Col. 4, lines 41 – 60 & Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14, the examiner notes that the examiner interprets “patch,” as the transfer or download of information from one electronic device to another electronic device, for example, the transfer of data between a computer and a mobile phone, furthermore the examiner notes that the second device has a Encryption/Decryption processor); and

- validating the patch during a boot operation of the wireless device prior to execution of the patch of the at least one microcode instruction (Col. Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14, the examiner notes that the first device must recognize the hash of the second device before allowing it to store the transferred data, this is what the examiner considers as "validating the patch."),

wherein the validating comprises:

- validating a cryptographic key of the patch based on a hash of the cryptographic key that is stored in a one time programmable storage in a nonvolatile memory that is external to the cryptographic processor (Col. 5, lines 41 - 67

& Col. 6, lines 1 - 14).

Claim # 15. The method of claim 14 further comprising receiving a signature of the patch, wherein the validating of the patch comprises:

- generating a digest of the patch using a hash unit within the cryptographic processor (Col. 5, lines 50 - 67 & Col. 6, lines 1 - 14, the examiner notes to one of ordinary skill in the art, a hashing of data, will produce a digest or digital fingerprint);

- decrypting the received signature of the patch to generate a decrypted received signature (Col. 6, lines 10 – 14, the examiner notes that decryption is used to decrypt the data and the hash);

- comparing the decrypted received signature to the generated digest (Col. 6, lines 10 – 14, the examiner notes that the first device to one ordinary skill in the art, would have to have the means to verify the hash and encryption/decryption scheme); and

- validating the patch if the decrypted received signature equals the generated digest (Col. 6, lines 10 – 14, the examiner notes that the first device to one ordinary skill in the art, would have to have the means to verify the hash and encryption/decryption scheme)

Claim # 16. The method of claim 14, wherein

- receiving the patch of the at least one microcode instruction stored in the nonvolatile memory within the cryptographic processor in the wireless device comprises receiving the patch from a nonvolatile memory external to the cryptographic processor (Col. Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14 & Figures #2a, 2b, the examiner notes that the first device is a computer and the second device is mobile telephone, and the first device sends data to the second device for encryption and decryption purposes).

Claim # 17. The method of claim 14, wherein

- receiving the patch of the at least one microcode instruction stored in the nonvolatile memory within the cryptographic processor in the wireless device comprises receiving a patch of a part of the microcode instructions in the nonvolatile memory, wherein the patch includes at least one patch flag that identifies the part of the microcode instructions to be patched (Col. Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14 & Figures #2a, 2b, the examiner notes that the first device is a computer and the second device is mobile telephone, and the first device sends data to the second device for encryption and decryption purposes, furthermore the examiner interprets the claim limitation “patch flag,” merely as the second device receive unencrypted data from the first device, and the second device recognizes that the first device want the data to by encrypted).

Claim # 18. The method of claim 14 further comprising

- loading a segment of the patch into a volatile memory within the cryptographic processor after at least one microcode instruction within the segment is to be executed in place of a microcode instruction stored in the nonvolatile memory within the cryptographic processor (Col. Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14 & Figures #2a, 2b, the examiner notes that the first device is a computer and the second device is mobile telephone, and the first device sends data to the second device for encryption and decryption purposes).

Claim # 23. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

- receiving a patch of at least one microcode instruction stored in nonvolatile memory within a cryptographic processor in a wireless device(Col. 2, lines 20 – 25 & Col. 2, lines 31 – 36 & Col. 3, lines 14 – 53 & Col. 4, lines 41 – 60 & Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14, the examiner notes that the examiner interprets “patch,” as the transfer or download of information from one electronic device to another electronic device, for example, the transfer of data between a computer and a mobile phone, furthermore the examiner notes that the second device has a Encryption/Decryption processor); and

- validating the patch during a boot operation of the wireless device prior to execution of the patch of the at least one microcode instruction (Col. Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14, the examiner notes that the first device must recognize the hash of the second device before allowing it to store the transferred data, this is what the examiner considers as "validating the patch."),

wherein the validating comprises:

- validating a cryptographic key of the patch based on a hash of the cryptographic key that is stored in a one time programmable storage in a nonvolatile memory that is external to the cryptographic processor (Col. 5, lines 41 - 67 & Col. 6, lines 1 - 14).

Claim # 24. The machine-readable medium of claim 23 further comprising receiving a signature of the patch, wherein the validating of the patch comprises:

- generating a signature of the patch using a hash unit within the cryptographic processor (Col. 5, lines 41 – 64, the examiner notes that the hash value v2 and device identifier ID2 are used as a signature to identify a key for encryption and decryption of the transferable data);

- comparing the received signature to the generated signature (Col. 5, lines 41 – 64); and

- validating the patch if the received signature equals the generated signature(Col. 5, lines 41 – 64).

Claim # 25. The machine-readable medium of claim 23, wherein

- receiving the patch of the at least one microcode instruction stored in the nonvolatile memory within the cryptographic processor in the wireless device comprises receiving the patch from a nonvolatile memory external to the cryptographic processor (Col. Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14 & Figures #2a, 2b, the examiner notes that the first device is a computer and the second device is mobile telephone, and the first device sends data to the second device for encryption and decryption purposes).

Claim # 26. The machine-readable medium of claim 23 further comprising

- loading a segment of the patch into a volatile memory within the cryptographic processor after at least one microcode instruction within the segment is to be executed in place of a microcode instruction stored in the nonvolatile memory within the cryptographic processor(Col. Col. 5, lines 17 – 22 & Col. 6, lines 10 – 14 & Figures #2a, 2b, the examiner notes that the first device is a computer and the second device is mobile telephone, and the first device sends data to the second device for encryption and decryption purposes).

Claim(s) 27 – 32 are rejected under 35 U.S.C. 102(e) as being taught by Zotto et al. (US Patent # 2004/0009815).

Zotto teaches:

Claim # 27. A system comprising:

- a FLASH memory to store a hash in a one time programmable storage (Paragraph: 0035 & 0019 & 0039),

wherein

- the hash is of a cryptographic key associated with a patch of the at least one microcode instruction (Paragraph: 0035);

and

a cryptographic processor comprising:

- a nonvolatile memory to store the at least one microcode instruction to be patched (Paragraph: 0035 & 0019 & 0039 & 0139);
- a number of cryptographic units(Paragraph: 0136); and
- a controller to cause at least one of the number of cryptographic units to validate the patch based on the cryptographic key and the hash of the cryptographic key (Paragraph: 0137 & 0155, the memory processor executes the exchange of data between the components within a computer).

Claim # 28. The system of claim 27, wherein

- the FLASH memory is to store a signature of the patch based on the cryptographic key, wherein the controller is to cause at least one of the number of cryptographic units to validate the patch based on the signature (Paragraph: 0035, the examiner notes that the examiner interprets "signature of the patch," as the game console and the content server, having matching content digests, which authenticates the requested content or patch).

Claim # 29. The system of claim 27, wherein

- the nonvolatile memory is a read only memory (Paragraph: 0019 & 0039).

Claim # 30. The system of claim 27, wherein

- the cryptographic processor further comprises a volatile memory, wherein the controller is to cause the patch to be loaded into the volatile memory after the patch is validated (Paragraph: 0136 & 0139 & 0155).

Claim # 31. The system of claim 30, further comprising

- an application processor to generate a primitive instruction related to a cryptographic operation, wherein the controller is to retrieve the at least one microcode instruction related to the primitive instruction from the patch loaded into the volatile memory or from the nonvolatile memory (Paragraph: 0136, the examiner notes that the gaming console and content server both have cryptographic processors and application processors (i.e. non - cryptographic processors)).

Claim # 32. The system of claim 31, further comprising

- a shared volatile memory, wherein the shared volatile memory is partitioned into a public section and a private section, wherein the public section is accessible by the cryptographic processor and the application processor, and wherein the private section is accessible by the cryptographic processor and not the application processor (Paragraph: 0139 & 0155, the examiner notes that the application processor, executes non – cryptographic operations that do not involve encryption and decryption of content and digest, thus the cryptographic processor does).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANT B. SHAIFER HARRIMAN whose telephone number is (571)272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Dant B Shaifer - Harriman /
Examiner, Art Unit 2134

07/14/2008

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2134